ZigBee in Industry

Bachelor Thesis Performed in Computer Engineering

by

Andreas Wettergren

LiTH-ISY-EX--07/0335--SE
Linköping 2007

ZigBee in Industry

Bachelor Thesis Performed in Computer Engineering
at Linköping Institute of Technology

by

Andreas Wettergren

LiTH-ISY-EX--07/0335--SE

Supervisors: Michael Josefsson, Erik Karlsson
Examiner: Michael Josefsson
Linköping 2007-08-29

Presentation Date

2007-08-29

Publishing Date (Electronic version)

2007-10-31

Department and Division

Department of Electrical Engineering

Language

_X_ English
___ Other (specify below)

Number of Pages
65

Type of Publication

___ Licentiate thesis
_X_ Degree thesis
_X_ Thesis C-level
___ Thesis D-level
___ Report
___ Other (specify below)

ISBN (Licentiate thesis)

ISRN: LiTH-ISY-EX--07/0335--SE

Title of series (Licentiate thesis)

Series number/ISSN (Licentiate thesis)

URL, Electronic Version
http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-10061

Publication Title
Zigbee in Industry

Author(s)
Andreas Wettergren

Abstract
This Bachelor of Science thesis has the primary objective to investigate whether or not the wireless technology ZigBee is suitable for industry usage. The thesis work has been done in collaboration with Binar Elektronik AB (Trollhättan, Sweden). The background story for this collaboration is that Binar is interested in finding out if ZigBee is suitable for one of their upcoming products.

The thesis is divided into four main parts, beginning with a researching part concerning ZigBee as a concept and a market research on ZigBee hardware. The thesis continuous with a specialization towards one ZigBee hardware, the ZigBee module from MaxStream called Xbee. The Xbee module was chosen based on the result from the market research. This part also describes the code that has been developed for the Xbee module, which main purpose is to simplify communication with the module.

The next part of the thesis contains a number of different field tests that show how ZigBee communication is affected in different environments. This part also includes a range test with the Xbee module. The last part of the thesis contains the final results and conclusions, which clearly show that the ZigBee technology, and Xbee in particular, has a potential to satisfy the requirements for a wireless system in an industrial environment. This conclusion concerning the industrial usability of ZigBee should however be seen in the light of this particular thesis work, making this conclusion viable only for the field test environments.

Number of pages: 65

Keywords
ZigBee, Industry, Xbee, Wireless, C Programming, API, Field test

ABSTRACT

This Bachelor of Science thesis has the primary objective to investigate whether or not the wireless technology ZigBee is suitable for industry usage. The thesis work has been done in collaboration with Binar Elektronik AB (Trollhättan, Sweden). The background story for this collaboration is that Binar is interested in finding out if ZigBee is suitable for one of their upcoming products.

The thesis is divided into four main parts, beginning with a researching part concerning ZigBee as a concept and a market research on ZigBee hardware. The thesis continuous with a specialization towards one ZigBee hardware, the ZigBee module from MaxStream called Xbee. The Xbee module was chosen based on the result from the market research. This part also describes the code that has been developed for the Xbee module, which main purpose is to simplify communication with the module.

The next part of the thesis contains a number of different field tests that show how ZigBee communication is affected in different environments. This part also includes a range test with the Xbee module. The last part of the thesis contains the final results and conclusions, which clearly show that the ZigBee technology, and Xbee in particular, has a potential to satisfy the requirements for a wireless system in an industrial environment. This conclusion concerning the industrial usability of ZigBee should however be seen in the light of this particular thesis work, making this conclusion viable only for the field test environments.

Sammanfattning

Den här C-uppsatsens mål är att undersöka om den trådlösa tekniken ZigBee är lämplig att använda i en industriell miljö. Arbetet med uppsatsen har utförts i Trolhättan (Sverige) i företaget Binar Elektronik AB:s lokaler. Bakgrunden till detta samarbete är att Binar vill veta om ZigBee är ett lämpligt val för en av deras framtida produkter.

Uppsatsen är uppdelad i fyra delar, där den första och inledande delen översiktligt beskriver begreppet ZigBee. Den här delen innehåller även en marknadsundersökning rörande ZigBee-hårdvara. Uppsatsen fortsätter sedan med nästa del där en specialisering mot en specifik ZigBee-hårdvara tar vid. Den ZigBee-modul som valdes kallas Xbee och den blev utvald baserat på resultatet från marknadsundersökningen. Den här delen beskriver även den kod som utvecklats för att på ett effektivt sätt kommunicera med Xbee-modulen.

Uppsatsens tredje del består av ett antal praktiska tester i olika miljöer, vars mål är att påvisa vilka styrkor och svagheter som ZigBee-tekniken har i respektive miljö. Den här delen innehåller även ett räckviddstest av Xbee-modulen. Den sista och avslutande delen innehåller uppsatsens resultat och slutsatser. Dessa slutsatser visar tydlig att Xbee-modulen, och dess ZigBee-tekniken, har stor potential att uppfylla de krav som ställs på ett trådlöst system i en industriell miljö. Det måste dock noteras att denna slutsats ej bör tas ur sitt sammanhang och att den således endast är giltig för de testmiljöer som den här uppsatsen behandlat.

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my gratitude towards my supervisor, lecturer Michael Josefsson at Linköping University, for the support he has given me throughout this whole project. I would also like to thank Binar Elektronik AB for giving me the opportunity to do my research on-site in Trollhättan.

Finally I would like to thank my family, my trustworthy frisbee discs, and all of my great friends for the support they gave me when times got rough.

Table of Contents

1 Introduction....1
- 1.1 Background....1
- 1.2 Goal....1
- 1.3 Method....1
- 1.4 Outline....2

2 Research about ZigBee....3
- 2.1 ZigBee Alliance....3
- 2.2 IEEE 802.15.4....3
- 2.3 ZigBee vs 802.15.4....4
- 2.4 Certification....5
- 2.5 Profiles....5
- 2.6 ZigBee market research....5

3 Hardware....9
- 3.1 ZigBee module....9
- 3.2 Microcontroller....11

4 Software....13
- 4.1 AVR Studio (IDE)....13
- 4.2 Xbee basics....14
- 4.3 API for Xbee....15

5 Wireless communication....19
- 5.1 Transmit power....19
- 5.2 Receiver sensitivity....19
- 5.3 Spread spectrum....20
- 5.4 Duplex modes for Xbee....22
- 5.5 Antenna types....22
- 5.6 Swedish National Post and Telecom Agency (PTS)....23
- 5.7 Industrial, Scientific and Medical (ISM)....23

6 Field tests....25
- 6.1 Loopback test....25
- 6.2 Field test setup....26
- 6.3 Field test basics....27
- 6.4 Test cases....29
- 6.5 Range tests....38

7 Conclusions....41
- 7.1 Appropriate for industrial usage?....41

8 Further work....43

Appendices
- A Code listing
- B Requirement specification
- C Market research table

List of Figures

Figure 2.1: Interconnection overview of IEEE 802.15.4 and ZigBee....3
Figure 2.2: Mesh network....4
Figure 2.3: Alternative route....4
Figure 3.1: Xbee development board (USB)....11
Figure 3.2: Atmel development board (AVR STK500)....12
Figure 4.1: AVR Studio....13
Figure 4.2: API Framework....15
Figure 5.1: Spread Spectrum....20
Figure 5.2: IEEE 802.15.4 channels for Xbee (All rights reserved to Digi International Inc.) 21
Figure 5.3: Unidirectional antenna (Parabolic)....22
Figure 5.4: Omni-directional antenna....22
Figure 6.1: Master (loopback test)....26
Figure 6.2: Slave (loopback test)....26
Figure 6.3: Field test setup (loopback test)....27
Figure 6.4: Office wall....29
Figure 6.5: Sheet metal wall....30
Figure 6.6: Bluetooth....31
Figure 6.7: ZigBee loopback....32
Figure 6.8: Microwave oven....33
Figure 6.9: Industry environment....34
Figure 6.10: Industry robot....35
Figure 6.11: Noise-free environment....36

List of Tables

Table 2.1: Market research....7
Table 3.1: Xbee comparison....9
Table 6.1: PER example....28
Table 6.2: Summary of field test results....37
Table 6.3: Maximum range....38

TERMINOLOGY

Abbrevation	Explanation
ACK	Acknowledge
AES	Advanced Encryption Standard
API	Application Programming Interface
APL	Application Layer (OSI))
ASCII	American Standard Code for Information Interchange
CCA	Clear Channel Assessment
dBi	Decibel Isotropic
dBm	Decibel referenced to one milliwatt
DSSS	Direct-Sequence Spread Spectrum
EIRP	Equivalent Isotropically Radiated Power
GCC	GNU Compiler Collection
GNU	GNU's Not Unix
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.15.4	MAC and PHY specification for Low-Rate Wireless Personal Area Networks
ISM	Industrial, Scientific and Medical
ITU	International Telecommunication Union
JTAG	Joint Test Action Group
kbit/s	Kilobits per second
MAC	Medium Access Control Layer (OSI)
NWK	Network Layer (OSI)
OSI	Open System Interconnection (Network model)
PCB	Printed Circuit Board
PER	Packet Error Rate
PHY	Physical Layer (OSI)
PTS	Swedish National Post and Telecom Agency
RF	Radio Frequency
RS-232	Recommended Standard 232 (Electrical specification)
RSSI	Received Signal Strength Indicator
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

1 Introduction

This introductory chapter describes the project's background story, the goal of the project, the method that has been used and finally an outline of all chapters.

1.1 Background

This thesis is the result of a final project of a Bachelor of Science in Computer Engineering. It is done in collaboration with Binar Elektronik AB, hereafter referred to as Binar. The background to this project is that Binar wants to investigate the possibility of using a wireless technology in an upcoming product. The wireless technology that has been selected for evaluation is called ZigBee.

1.2 Goal

The goal of this project is to investigate whether or not ZigBee is suitable for industry usage. The result of this investigation will supply Binar, and the reader of this thesis, with a well-founded conclusion concerning this matter. The project is mainly focused on the Swedish market as this is the introductory market for a potential product.

1.3 Method

This project is divided into four main parts:

1. **Research** – This part acknowledges the different aspects of the ZigBee standard and includes a comparison between different types of ZigBee hardware. This comparison is used in the next part of the project, the specialization towards one type of ZigBee hardware.
2. **Specialization** – In this part the most suitable ZigBee hardware is used as a base for the rest of the project. This part also describes the code that has been developed for utilizing the chosen hardware in an efficient way.
3. **Field tests** – This part of the project contains a number of different test cases that show how ZigBee communication is affected in different environments. The field tests is a combination of previously developed code, from part two, and code specialized for the field tests. The field tests main concern is how many packets that is lost due to increased levels of interference from different types of noise sources, e.g. microwave ovens and Bluetooth® devices[1]. This part also includes a range test with the module used in the field tests.
4. **Results and conclusions** – This part concludes the whole project and takes into account all results from the preceding parts of the project.

Note: As a base for this project a requirement specification from Binar is used. (See Appendix B Requirement specification.

1 Bluetooth is a registered trademark of Bluetooth SIG.

1.4 Outline

This outline briefly describes the chapters of this thesis:

- **Chapter 2 — Research about ZigBee:** Overview of the ZigBee standard and a market research on ZigBee hardware.
- **Chapter 3 — Hardware:** Describes the hardware used in this project.
- **Chapter 4 — Software:** Describes the software used in this project.
- **Chapter 5 — Wireless communication:** Describes the basics concerning wireless communication, with a special focus on ZigBee communication.
- **Chapter 6 — Field tests:** Describes the field tests that has been performed with the ZigBee modules.
- **Chapter 7 — Conclusions:** The final conclusions of this project.
- **Chapter 8 — Further work:** A list of suggestions that can simplify further research.

2 Research about ZigBee

This chapter begins with an overview of the ZigBee standard. The overview explains the role of the ZigBee Alliance, the connection between ZigBee and 802.15.4 and issues concerning networking, security and certification.

The second part of this chapter is dedicated to a market research on ZigBee hardware. The goal of the market research is to get an overview of the currently available ZigBee hardware and based on that choose a suitable hardware for this project. The market research is focused on the most important aspects of the hardware, for example the receiver sensitivity, maximum transmit power and which frequency band that is used.

2.1 ZigBee Alliance

ZigBee Alliance is an organization that has the aim to unite companies working with ZigBee, on a global level. ZigBee Alliance also handles changes and updates of the the steering document for ZigBee, the ZigBee Specification.

2.2 IEEE 802.15.4

The MAC and PHY-layer of the ZigBee standard is based on the wireless standard IEEE 802.15.4. The interconnection between the layers is depicted in figure 2.1.

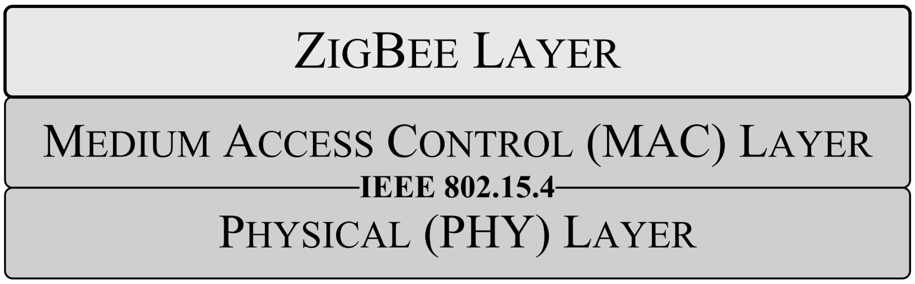

Figure 2.1: Interconnection overview of IEEE 802.15.4 and ZigBee

The most important characteristics of the standard[2] are the following:

- Over-the-air data rates of up to 250 kbit/s.
- Peer-to-peer and star network capability.
- 16-bit or 64-bit addressing modes.
- Reliable transfer protocol (based on ACK[3]).
- Low power consumption.
- Link Quality Indication (LQI).
- 16 channels on the 2450 MHz band, 10 channels on the 915 MHz band.

Note: ZigBee is not bound to implement all of the functionality that the IEEE 802.15.4-layers specifies[4]. The reason for this not-so-strict policy is that it makes it possible to implement ZigBee

2 IEEE Std. 802.15.4-2003, ISBN 0-7381-3677-5, Chapter 5 General description
3 4.2.4 Packet acknowledge (ACK)
4 ZigBee Specification 2006, Document 053474r13, Annex D MAC and PHY Sub-Layer Clarifications

without having to use more code memory than needed for the implementation.

2.3 ZigBee vs 802.15.4

This is the level where the difference between ZigBee and IEEE 802.15.4 becomes visible, as ZigBee adds new functionality on top of the existing IEEE 802.15.4 framework. The most important extra features, compared to IEEE 802.15.4, are the following:

- Support for mesh[5] networks.
- Stronger security (In most cases AES-128 bit, see *2.6 ZigBee market research*.

2.3.1 Mesh

A mesh network has the following characteristics:

- Every node is capable of connecting directly to all of its neighboring nodes.
- Every node is capable of routing traffic to and from all of its neighboring nodes.
- The network is self-forming. This means that new nodes is automatically added to the network without the need for manual configuration.
- The network is self-healing. This means that the network automatically adjust the routes to and from nodes if the network changes, for example when a node disappears from the network.

These characteristics makes a mesh network very robust, especially put in comparison with a regular star network that is dependent on a single connection point. It must however be noted that a mesh network can have single points of failure in a single connection point, but for a typical mesh network this is not the case. Figure 2.2 illustrates a typical mesh network and figure 2.3 shows how the mesh network dynamically adapts itself when a link is lost.

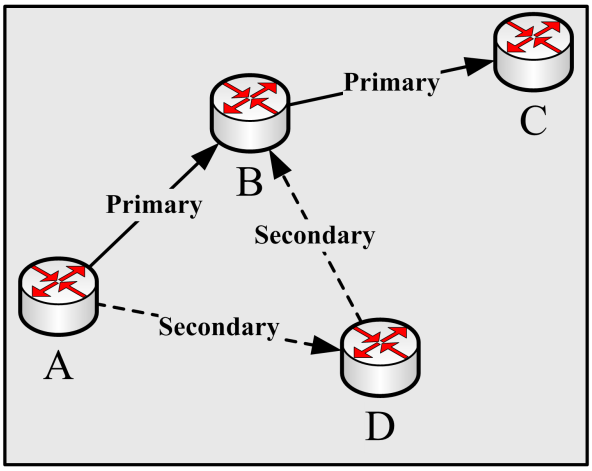

Figure 2.2: Mesh network

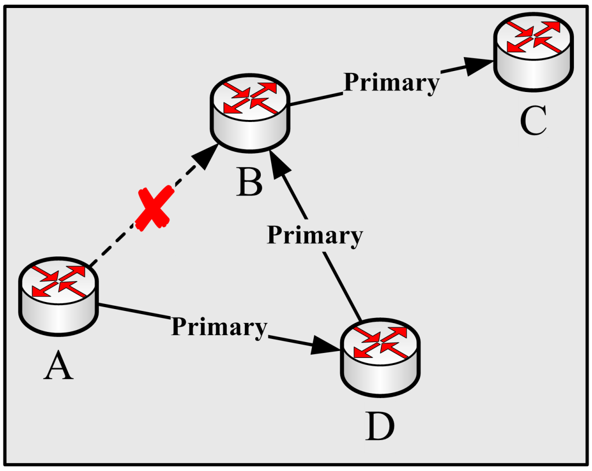

Figure 2.3: Alternative route

5 ZigBee Specification 2006, Document 053474r13, 1.1.4 Network Topology

2.3.2 Security

Security issues in ZigBee is addressed in the ZigBee specification and has security mechanisms on three layers, MAC, NWK and APL. For more detailed information about the security mechanisms in ZigBee, refer to chapter 4 of the ZigBee specification[6].

2.3.2.1 Virus issues

There exist no known viruses at the moment, but there is always a risk, especially if the ZigBee technology becomes widely used in the future.

2.4 Certification[7]

There exists three types of certifications for ZigBee, *ZigBee Complaint Platform (ZCP)*, *ZigBee Network Capable (ZNC)* and *ZigBee Certified Product*. There is also special restrictions concerning the use of the word *ZigBee* and the use of the *ZigBee logotype*. The cost for a certification is decided by the test providers, currently NTS Corporation or TUV Rheinland Group. A description of the different types of certifications can be found on the ZigBee Alliance website[8].

For clarity: If using a product that is *ZigBee Certified* no certification is needed by the end user, as long as the product is used in conjunction with how the product has been certified. The use of the name *ZigBee* and *ZigBee logotype* is decided on a per-product basis and is regulated by the ZigBee Alliance.

2.5 Profiles

One of the things the ZigBee Alliance supplies is specifications of how a ZigBee product should be constructed to achieve maximum interoperability with other ZigBee products. The way this is done is through the term *Profiles*[9]. A profile specifies how ZigBee communication is to take place between ZigBee nodes, as a way to make ZigBee modules from different vendors interoperable with each other.

2.6 ZigBee market research

In order to wisely choose a ZigBee hardware for this project a market research has been performed. This market research consists of a comparison between the different ZigBee chips/products available today[10].

6 ZigBee Specification 2006, Document 053474r13, Chapter 4 Security Services Specification
7 Because of the limited time for this thesis work and the complexity associated with the certifications this thesis will not dig deeper into the different types of certifications.
8 ZigBee Alliance website — http://www.zigbee.org (2007-08)
9 ZigBee Specification 2006, Document 053474r13, 2.3.1 Creating a ZigBee Profile
10 Because of the increasing development of new ZigBee chips it is not feasible to list every single chip, but the most used chips are covered in the comparison.

2.6.1 Considerations

This market research focuses on the following general aspects of the different ZigBee chips/products:

- Which **ZigBee-version** is used?
- Which **ZigBee stack** is used?
- Is **mesh networking** supported?
- Is there special support for **positioning**?
- Which **frequency bands** are supported?
- Which **chip** is used?
- What is the **price** of the chip/product?
- Is there support for **encryption**?
- How **sensitive** is the **receiver**?
- What is the maximum **transmit power**?

Apart from these general aspects two project-specific aspects is also considered, namely:

- Can the ZigBee hardware be delivered in time for the implementation part of this project?
- Is the hardware out-of-the-box ready for basic ZigBee networking?

These two aspects is of great importance as this project has a deadline that must be meet. The hardware must be delivered in time and be out-of-the-box ready for ZigBee networking. The fulfillment of these two aspects is vital for this project.

Note: For more detailed information concerning the wireless aspects, see chapter 5 Wireless communication.

2.6.2 Comparison table

Table 2.1 summarizes the most essential parts of the market research. The full table is available in Appendix C Market research table.

Table 2.1: Market research

Products					
Manufacturer	**Product name (chip)**	**ZigBee-version**	**Receiver Sensitivity**	**Transmit Power (Maximum)**	**Price***
Integration UK	IA OEM-DAMD1 2400 (OKI ML7065)	2006	−90 dBm	0 dBm	$49
MaxStream	**Xbee (MC13193)**	**2004**	**−100 dBm (Xbee-PRO)**	**+18 dBm (Xbee-PRO)**	**$19**
Renesas	RZB-CC16C-ZDK (Chipcon / ZMD)	2006	N/A	N/A	N/A

Chip only					
Manufacturer	**Chip**	**ZigBee-version**	**Receiver Sensitivity**	**Transmit Power (Maximum)**	**Price***
Chipcon / Texas Instruments	CC2420/30/31	2006	−95 dBm (CC2420)	0 dBm (CC2420)	$6
Ember	EM250/260	2004	−98 dBm (EM260)	+5 dBm (EM260)	$7
Freescale	MC1319x,MC1320x, MC1321x	2004	−92 dBm (MC1321x)	+3 dBm (MC1321x)	$4
Helicomm	IP-Link 1000/122x	2004	−94 dBm (IP-Link 1220)	+10 dBm (IP-Link 1220)	$25
Jennic	JN5121/513x	2004	−97 dBm (JN513x)	+3 dBm (JN513x)	£20
MeshNetics	ZDM-A1281-xx	2006	−101 dBm (ZDM-A1281-xx)	+3 dBm (ZDM-A1281-xx)	$21
Microchip Inc.	MRF24J40	2004	−91 dBm (MRF24J40)	0 dBm (MRF24J40)	$3
OKI Semiconductors	ML7065	2006	−90 dBm (ML7065)	+3 dBm (ML7065)	$4
RadioPulse Inc.	MG2400/LM2400	2004	−99 dBm (LM2400)	+14 dBm (LM2400)	$10

Stack only					
Manufacturer	**Compliant chips**	**ZigBee-version**	**Receiver Sensitivity**	**Transmit Power (Maximum)**	**Price**
Korwin	JN5121/CC2420	2004	Chip dependent	Chip dependent	N/A
Institute for Information Industry	CC2430/JN5121	2004	Chip dependent	Chip dependent	N/A
AirBee	N/A	2006	Chip dependent	Chip dependent	N/A

Price*: Average price from random supplier

2.6.3 Discussion

This section discusses the result of the market research.

2.6.3.1 Similarities

The markets research shows that there are a few characteristics that is common for all products and chips that has been considered[11]:

- Mesh networking is supported.
- AES encryption is available (in software or hardware).
- Uses the 2,4 GHz band for wireless communication.

This result implicates that if the only concern when choosing ZigBee hardware is these three characteristics, then any of the chips/products will suffice.

2.6.3.2 Differences

Apart from the similarities listed in *2.6.3.1 Similarities* the different ZigBee chips/products differ in many aspects, some more than others. The list below shows the differences:

- The ZigBee version is either **2004** or **2006**.
- The ZigBee stack is in most cases vendor specific.
- **Positioning** of ZigBee nodes has hardware support (beta) from Chipcon/TI. Institute for Information Industry has a stack that supports positioning.
- Helicomm is the only manufacturer that has a radio module for the **915 Mhz** band.
- Prices for the ZigBee hardware ranges from **$3** up to **$49**.
- The receiver sensitivity ranges from **−90 dBm** down to **−101 dBm**.
- The maximum transmit power ranges from **0 dBm** up to **+18 dBm**.

2.6.4 Conclusion

Based on the considerations (*2.6.1 Considerations*) the ZigBee product from MaxStream, called Xbee, has been selected as the hardware that is to be used in the rest of the project. The main reasons for choosing the Xbee are the following:

- Straightforward out-of-the-box features (Standard UART and API mode[12]).
- Reasonable price.
- Very good wireless performance.
- Delivery of the hardware in due time (Late delivery of the hardware would have jeopardized the whole project).

11 Appendix C Market research table
12 4.3 API for Xbee

3 Hardware

This chapter covers the hardware used in this project, beginning with a comparison between the two types of ZigBee modules, Xbee-STD and Xbee-PRO. The chapter is then focused on issues concerning temperature ratings for the Xbee modules, as well as the problems with the ZigBee stack. As a response to the ZigBee stack problem a separate microcontroller is used, in this case a ATMega162 from Atmel. The chapter ends with a description of the microcontroller and the tools used to simplify the development process.

3.1 ZigBee module

The ZigBee modules that is used in this project is manufactured by MaxStream and is called Xbee. In its simplest form this module, paired with another module, works as a cable replacement (transparent mode[13]) for serial communication (UART). If this simple approach is too limiting for the application it is also possible to build up a mesh network consisting of up to 46 656 nodes[14].

The Xbee comes in two flavours, Xbee-STD and Xbee-PRO. Table 3.1 shows the major differences between them (see the Xbee Specification[15] for a more detailed version).

Table 3.1: Xbee comparison

Specification	Xbee-STD	Xbee-PRO
Transmit Power Output	1 mW (0 dBm)	60 mW (18 dBm)
Receiver Sensitivity	−92 dBm (1% PER)*	−100 dBm (1% PER)*
Transmit Current (typical)	45 mA (@ 3.3V)	215 mA (@ 3.3V, 18 dBm)
Idle / Receive Current (typical)	50 mA (@ 3.3V)	55 mA (@ 3.3V)
Number of Channels (DSSS)	16	12

***PER:** *Packet Error Rate*

Xbee-STD with chip antenna

Xbee-PRO with whip antenna

Note: In order to simplify the text in this thesis the term "Xbee" is used to describe both the Xbee-STD and the Xbee-PRO. The reason for this is that apart from the differences depicted in table 3.1 the two modules are considered interchangeable.

13 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13], 2.1.2 Transparent Operation
14 Xbee/Xbee-PRO ZigBee OEM RF Modules v8.x17 Beta [2007.01.022], figure 2-03: Maximum Network Depth
15 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13]

3.1.1 Temperature issues

The requirement specification states that the system must be functional in a surrounding environment that can be from −20 °C up to 60 °C. The Xbee module is specified to function properly within −40 °C to 85 °C, well above and below the required temperatures. It should however be noted that these figures does not take into account the heat dissipations from the Xbee module. For the highest temperature the margin is

$$85\,°C - 60\,°C = 25\,°C \quad (1)$$

and for the lowest temperature

$$-20\,°C - (-40)\,°C = 20\,°C \quad (2)$$

These figures are of great importance when designing the final system, for example the case design of the product. The reason for this is that if the casing is built without considering the effects of heat dissipation the temperature inside the product can exceed the limitations.

In order to design a product that can handle the heat dissipation effects from the hardware, in this case the Xbee, a heat dissipation figure is needed from the manufacturer. In most cases this figure can be found in the specification of the hardware, but this was not the case for the Xbee. As a next step towards finding this figure the manufacturer was contacted, but they had not done any testing concerning heat dissipation, so there existed no such figure.

Without this figure it is impossible to calculate the real heat dissipation, but some conclusions can be drawn from the following calculation. The calculation is based on the most power-hungry model, the Xbee-PRO.

Calculation:

The module is set to use maximum transmit power.

$Xbee_{MAX}$ = 60 mW
U = Supply voltage to the module
I = Transmit current for selected power level
P = U * I = Heat dissipation in watts

U = 3,3 V
I = 0,215 A
P = 3,3 V * 0,215 A = 0,7095 W ≃ 710 mW

This results in the following:

Maximum heat dissipation = P - $Xbee_{MAX}$ = 710 - 60 mW = 650 mW

3.1.1.1 Conclusion

With the above calculations and the temperature margins from (1) and (2) it seems unlikely that heat dissipation would be a problem when the maximum heat dissipation is 650 mW for the Xbee-PRO module. Their might be temperature issues if the Xbee module is housed inside a *very* small casing, with poor ventilation, but other than that there should be no problems.

3.1.2 Xbee development board

To make it easier to interface the Xbee module a development board has been used, one for each module. When the Xbee is mounted on the development board it enables an easy way of communicating with it, either over RS-232 or USB. Figure 3.1 shows the USB version of the development board.

Figure 3.1: Xbee development board (USB)

3.1.3 ZigBee stack problem

In the beginning of this project it was first decided that the microcontroller on the Xbee was to be used as a base for development. This seemed like a good idea at first, but along the way it became clear there was a problem with this approach, namely the ZigBee stack. The memory of the microcontroller on the Xbee was completely filled up with the ZigBee stack, so there was no space left for additional code. This left the project with two alternatives, either remove some of the ZigBee stack code, or go with an external microcontroller. The second option was selected.

3.2 Microcontroller

The microcontroller that is used in this project is ATMega162 from Atmel. It suits the project well as it has two serial ports (UART), which is of importance to the final part of the project, the integration with one of Binar's products. It should however be noted that *any* microcontroller with two serials ports could have been used in this project, instead of the ATMega162

3.2.1 Atmel development board

Once again a development board is used, the Atmel AVR STK500 (see figure 3.2). This development board has full support for the ATMega162 and it gives the developer a straightforward way of developing code for this platform.

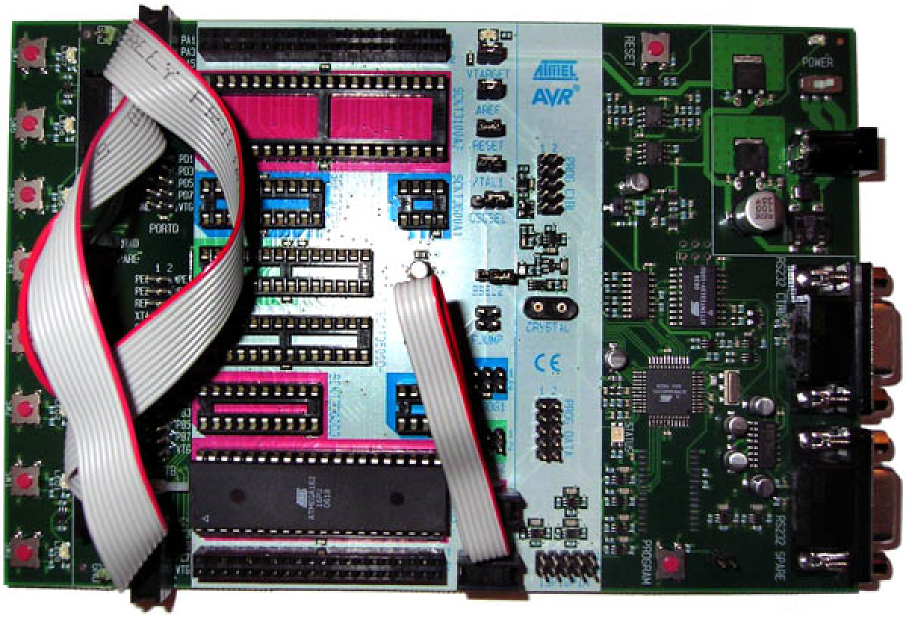

Figure 3.2: Atmel development board (AVR STK500)

3.2.2 AVR Dragon Debug Tool

In order to simplify the development process a good debug tool was needed, in this case the AVR Dragon from Atmel. The AVR Dragon is a powerful realtime debugger that enables single-stepping during runtime, which proved to be of significant importance during the developing process. It was especially useful when working with UART communication between the Xbee and the ATMega162.

The AVR Dragon connects to the ATMega162 via the JTAG interface, and to the PC via USB.

4 Software

This chapter covers the software used in this project, beginning with a description of the development tools. The chapter is then focused on some basic facts about the Xbee module that is needed to fully understand the rest of this thesis, for example issues concerning addressing and firmware versions.

The end of the chapter describes the code for the Application Programming Interface (API), which is used to interface the Xbee module. This section is an overview of the functions that has been implemented and it describes how each function is to be used in the context of the API.

4.1 AVR Studio (IDE)

The Integrated Development Environment (IDE) used for the ATMega162 is AVR Studio 4.13 (see figure 4.1 below).

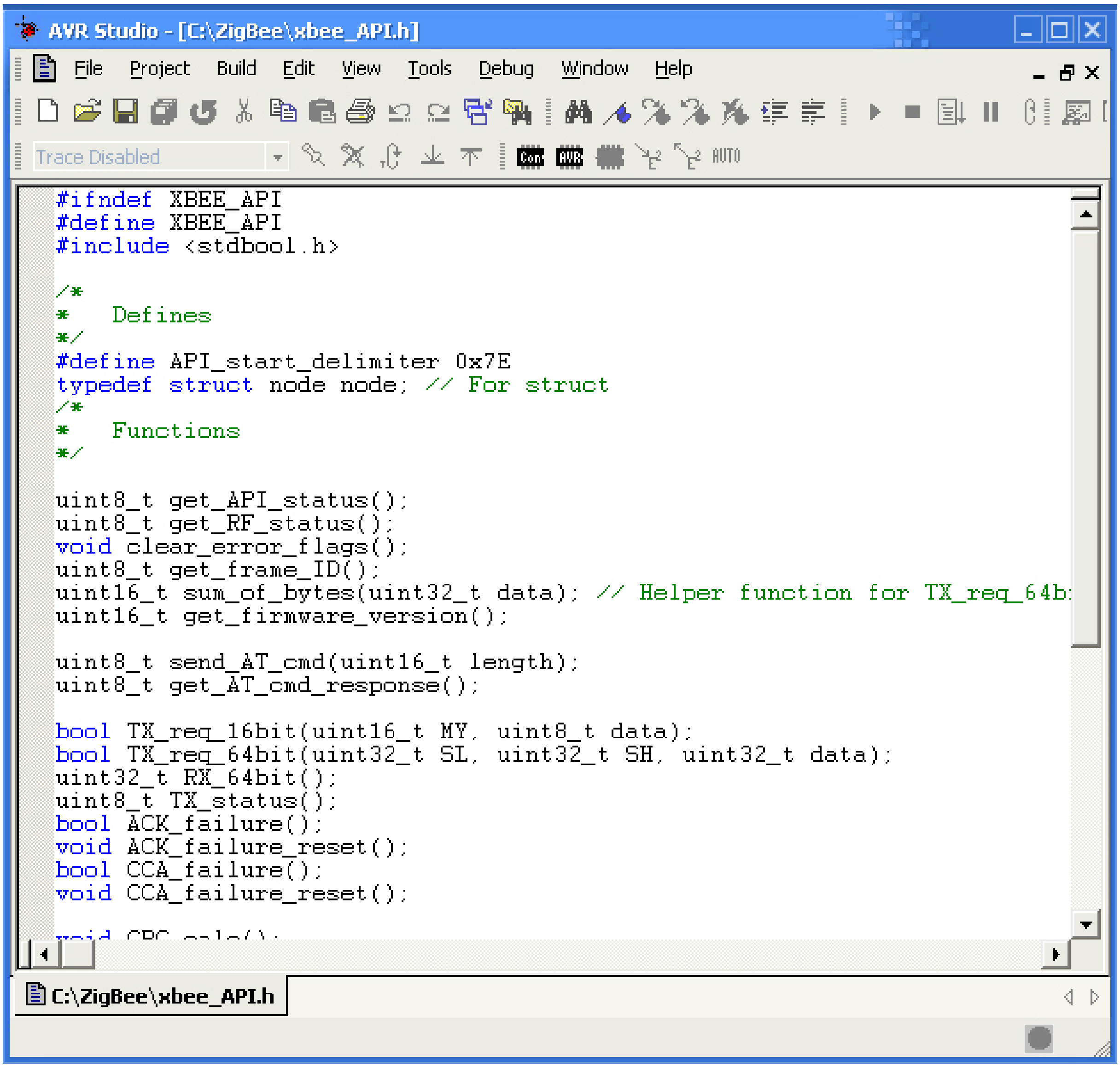

Figure 4.1: AVR Studio

4.1.1 WinAVR

Even before this project started it was obvious that it would not be possible (or at least very difficult) to write the software in assembly language. The alternative to writing in assembly is of course C, or maybe C++, so a compiler for C/C++ was clearly needed. In order to integrate a compiler for C/C++ into AVR Studio some third-party software was needed, in this case WinAVR. The WinAVR software is based on the GNU GCC compiler for C/C++ and is easily integrated with AVR Studio.

4.2 Xbee basics

This section describes some basic facts about the Xbee module that is needed to fully understand the rest of this thesis.

4.2.1 Addressing

There is two ways of addressing an Xbee module, by its 16-bit source address (software selectable) or by its unique IEEE 64-bit serial number[16]. The 64-bit serial number is assigned the module before it leaves the factory and can *not* be changed.

The 16-bit address simplifies communication with its shorter address, but it also introduces the risk of collisions if one particular address is assigned to multiple nodes within the same network. If the 64-bit serial number is used for addressing there is no problem with collisions, but it increases overhead in the communication.

4.2.2 Node identifier

The node identifier (NI) is a 20 character long ASCII string that is software selectable for every node. The node identifier is very useful because it simplifies addressing, instead of using the cryptic 16-bit/64-bit addresses directly the node identifier can be used to lookup the real addresses.

4.2.3 Received Signal Strength Indicator (RSSI)

The Received Signal Strength Indicator (RSSI) is a value that indicates how strong the wireless signal is. It is a logarithmic value in the range 0 dBm to −100 dBm, but it is however only accurate[17] between −40 dBm and the modules receiver sensitivity[18].

4.2.4 Packet acknowledge (ACK)

The use of packet acknowledge[19] (ACK) is needed to ensure a reliable communication scheme. For every packet sent from node A to node B an ACK is required from node B to node A. If node A receives the ACK then the sent packet was received correctly. On the other hand, if the ACK is not received something has gone wrong and suitable actions must be taken, like resending the initial packet.

16 ZigBee Specification 2006, Document 053474r13, 1.2.1.3 Entities
17 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13], page 39 — DB Command
18 5.2 Receiver sensitivity
19 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13], page 21 — Acknowledgement

4.2.5 Clear Channel Assessment (CCA)

Clear Channel Assessment[20] (CCA) is a technique for detecting noisy RF environments. Prior to transmitting a packet the module scans the RF environment for activity and if the RF environment is too clogged with noise the transmission is postponed to a later time (called the back-off period). After the back-off period another transmit request is performed, and this will hopefully lead to a successful transmission because of less noise in the RF environment the second time.

4.2.6 Xbee firmware

The Xbee modules can be used with two main types of firmware, *802.15.4* firmware or *ZigBee* firmware. The next two subsections describes the two firmwares in more detail.

4.2.6.1 802.15.4

The 802.15.4 firmware makes the module act as a standard 802.15.4 device. This makes the module capable of peer-to-peer communication and star networking, as specified in the IEEE 802.15.4 standard (see *2.2 IEEE 802.15.4*).

4.2.6.2 ZigBee

The ZigBee firmware makes the module act as a ZigBee device. With this firmware the module has support for both mesh networking and the standard 802.15.4 network techniques.

4.3 API for Xbee

In order to communicate with the Xbee module in an efficient way some sort of structured interface is needed, in this case called API – Application Programming Interface. The API is built on a frame-based protocol, consisting of the following parts, *Start Delimiter*, *Length of Frame Data*, *Frame Data*, and finally a *Checksum* (see figure 4.2 API Framework). This API frame is sent byte-wise via UART.

Start Delimiter + Length of Frame Data + Frame Data + Checksum

Figure 4.2: API Framework

For clarity: For a full specification of the API framework refer to the Xbee module documentation[21].

The subsections of this section describes the main parts that has been implemented of the API. For a full code listing, see Appendix A Code listing.

Note: This API is based on the 802.15.4 firmware and does *not* work with the ZigBee firmware, although some functions are exactly the same for the both firmwares. It is however fairly easy to implement an API for the ZigBee firmware based on the API for the 802.15.4 firmware.

20 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13], page 21 — CCA
21 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13], 3.4.1 API Frame Specification

4.3.1 Transmit packet with 64-bit addressing

Function name: `bool TX_req_64bit(uint32_t SL, uint32_t SH, uint32_t data)`
This function transmits a packet to a specific node, using 64-bit addressing.

4.3.2 Receive packet with 64-bit addressing

Function name: `uint32_t RX_64bit()`
This function receives a packet and reports the 64-bit address of the sender.

4.3.3 Packet Acknowledge (ACK)

Function name: `bool ACK_failure()`
This function checks if there has been any acknowledge (ACK) failures for packets sent via RF.
(See *4.2.4 Packet acknowledge (ACK)*)

4.3.4 Clear Channel Assessment (CCA)

Function name: `bool CCA_failure()`
This function checks if there has been any CCA failures.
(See *4.2.5 Clear Channel Assessment (CCA)*)

4.3.5 Serial number

Function name: `uint32_t get_serial_number(char select)`
This function reads out the serial number of the module.

4.3.6 Node identifier

Function name: `char* get_node_ID()`
This function reads out the 20 character ASCII string (node identifier).

Function name: `bool set_node_ID(char node_ID[])`
This function changes the node identifier value to a new value.

4.3.7 Node discovery

Function name: `uint8_t node_discovery()`
This function makes the Xbee module search for other Xbee modules in the vicinity and retrieves the following information about the discovered Xbee modules:

- Source address (MY)
- Serial number (SH,SL)
- RSSI value (DB)
- Node identifier (NI)

This information is stored in the memory of the microcontroller and can be read out at any time.

4.3.8 Node discover time

The node discover time is the limiting factor when doing a node discovery. If a relative short time is set, fewer nodes are discovered, and vice versa.

Function name: `uint8_t get_node_discover_time()`
This function reads out the the node discover time value.

Function name: `bool set_node_discover_time(uint8_t time)`
This function sets the node discover time value.

4.3.9 Transmit power level

Function name: `uint8_t get_power_level()`
This function reads out which transmit power level the module is set to.

Function name: `bool set_power_level(uint8_t level)`
This function sets the transmit power level to a new value.

4.3.10 Firmware version

Function name: `uint16_t get_firmware_version()`
This function reads out the firmware version of the module.

4.3.11 Save configuration

Function name: `bool save_changes()`
This function stores all the changes that has been made to the long-term memory of the Xbee module.

5 Wireless communication

This chapter describes the basics concerning wireless communication, with a special focus on ZigBee communication. The chapter starts off with discussions concerning the transmitting power and receiver sensitivity of wireless devices. The chapter continuous with channel usage issues and a discussion about the spread spectrum technology that is used by the Xbee.

The middle section of this chapter covers data rate issues with the Xbee, both internally and over-the-air. This section also describes the two main types of antennas, unidirectional and omni-directional.

The last part of this chapter covers the legal issues of Swedish radio communication and also includes a discussion of the license-free ISM band. The chapter ends with a discussion on how to select a combination of transmit power level and antenna, without violating the radio laws specified by the Swedish National Post and Telecom Agency (PTS).

5.1 Transmit power

The transmit power is an important aspect of wireless communication as it limits the range of the signal. A higher transmit power results in longer range in the same way as a lower transmit power results in shorter range. The relationship between transmit power and range is however *not* linear. This non-linear relationship has the effect that the transmit power must be increased by a factor of 4 in order to double the range.

The two Xbee modules differ significantly between maximum transmit power, where Xbee-PRO is the more powerful version (see *3.1 ZigBee module*). The transmit power level is software selectable in both modules. The Xbee-STD ranges from −10 dBm to 0 dBm and the Xbee-PRO ranges from 0 dBm to +18 dBm.

5.2 Receiver sensitivity

The receiver sensitivity decides how strong and clear the signal must be in order for the receiver to interpret the signal correctly. Suppose you have two receivers, one with high sensitivity and one with low sensitivity. If the signal is strong and clear there is hardly any difference between how the two receivers interpret the signal, but this is not the case when the signal becomes weak. The low sensitivity receiver will at a certain point loose the ability to interpret the signal correctly, while the high sensitivity receiver is still functional.

Another thing concerning the receiver sensitivity is the logarithmic dBm scale that is often used for expressing the levels of sensitivity. The modules used in this project have a receiver sensitivity of −92 dBm (Xbee-STD) and −100 dBm (Xbee-PRO). At first glance it does not seem that big a difference between them, but it is important to notice that it is a logarithmic scale, and that it makes a huge difference in practice! A 3 dB(m) increase in sensitivity makes the receiver roughly twice as sensitive in practice.

5.2.1 RSSI, sensitivity and throughput

The RSSI[22] value is a measurement of how strong the signal is and it proved to be very accurate when performing the range tests. The specified sensitivity level for the Xbee-PRO is −100 dBm which corresponds to a RSSI value of −100. The recorded RSSI values for the range tests showed that is was possible to receive packets in full speed all the way down to −100 dBm, but this was under perfect conditions. This close to the sensitivity threshold even the slightest interference would render the signal uninterpretable by the receiver. This is also true the other way around, a strong signal can withstand significant interference and still be interpreted correctly by the receiver.

5.3 Spread spectrum

Spread spectrum is a technology that spreads a narrowband signal over a much wider bandwidth than in the normal case. The technology also makes the radio signal more resistant to interference and therefore more reliable. The principle behind this technology is a usage of multiple channels for transmitting a single signal. This is of special importance to this project as the Xbee modules utilizes a spread spectrum technique called Direct-Sequence Spread Spectrum (DSSS).

The remaining sub-sections of this section covers the modulation and demodulation of a spread spectrum signal. It should however be noted that this is not an in-depth explanation of spread spectrum, it merely gives an understanding to the underlaying technology of the Xbee. For a more detailed explanation of the technology refer to "Spread Spectrum (SS) introduction" by Jan De Nayerlaan[23] .

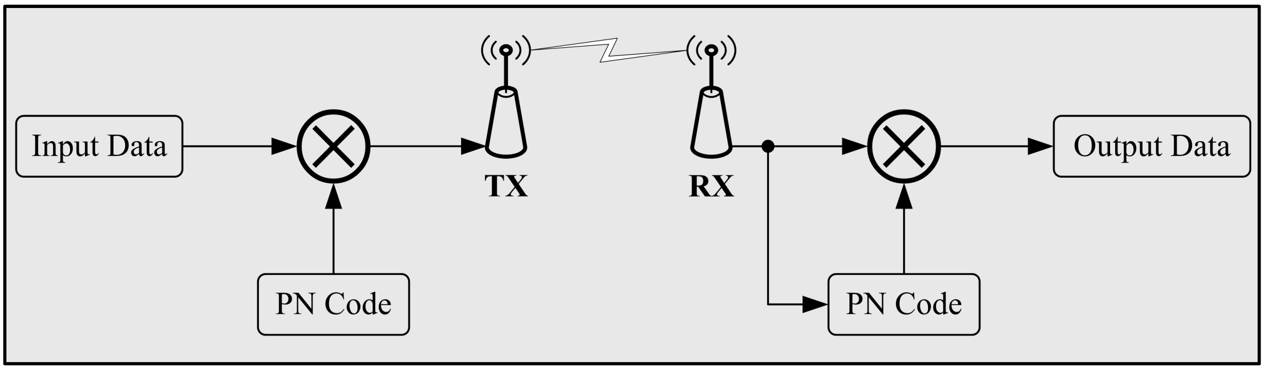

Figure 5.1: Spread Spectrum

5.3.1 Spread spectrum modulation

This spreading of the narrowband signal is done by multiplying the input data with a pseudo-noise (PN) code sequence[24]. This makes the output signal look like regular noise, but with the right demodulation technique the original data can be reproduced (see *5.3.2 Spread spectrum demodulation*).

A simplified explanation of this modulation is that the input data is encrypted with the PN code sequence and is then transmitted over-the-air looking like regular noise.

22 4.2.3 Received Signal Strength Indicator (RSSI)
23 Jan De Nayerlaan, *Spread Spectrum (SS) introduction*, version 2 Dec 1999
24 This code sequence is generated based on a pseudo-random number. Refer to "Spread Spectrum (SS) introduction" by Jan De Nayerlaan for more detailed information.

5.3.2 Spread spectrum demodulation

The spread spectrum signal, that looks like regular noise, needs to be demodulated in order for the receiver to interpret the signal correctly. This demodulation is done by multiplying the incoming signal with the same PN code sequence that the signal was modulated with. This also implicates that the PN code sequence must be shared between all devices that want to communicate using the spread spectrum technique. Once again, if explaining this with cryptology terms it means that spread spectrum is using a shared-key cryptology scheme.

5.3.3 Spread spectrum side-effects on channel usage

The usage of DSSS has some side-effects that needs to be considered when choosing which channels to utilize for radio communication. In a non-spread spectrum technique there exist almost no interference between different channels as the signal is concentrated to one channel. Spread spectrum techniques, on the other hand, spreads the signal on multiple channels. One channel is called the *center channel* and this is were the signal originates from. This has however a side-effect, subcarriers of the center channel spreads to neighboring channels and cause interference on these channels. The graph in figure 5.2 shows how neighboring signals is affected by the subcarriers, in this case from a signal with an amplitude of 0 dBm.

From a practical point of view this makes it problematic to use all available channels concurrently, at least if interference-free channels is needed. As stated earlier the Xbee modules utilizes DSSS and this technique has the side-effects described above. The Xbee-STD and the Xbee-PRO differ in how they use channels, Xbee-STD has 16 channels and Xbee-PRO 12 channels. The difference can be explained by the higher transmit power of the Xbee-PRO, as this most likely will increase the overhearing (the subcarriers has a higher amplitude). The lowest channel and the three highest channels (B, 18, 19, 1A in figure 5.2) is not available when using the Xbee-PRO[25].

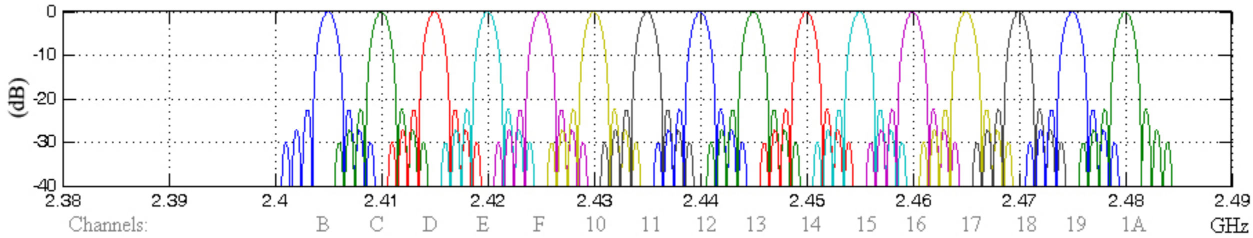

Figure 5.2: IEEE 802.15.4 channels for Xbee (All rights reserved to Digi International Inc.)

5.3.4 Data rates

Over-the-air data rates for the Xbee is 250 kbit/s, but because of the limitations of the UART on the Xbee the highest possible speed is 115,2 kbit/s.

The over-the-air data rate for the Xbee is fixed at 250 kbit/s independent of what the signal strength is. This means that if the receiver is unable to interpret the signal correctly, because of a weak signal, there are no measures to enhance the signal. A contrasting example to this can be found in the IEEE standard 802.11[26] (WLAN), in which the data rate is lowered by changing the modulation type, as a response to a weaker signal.

25 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13], table 3-02 Xbee/Xbee-PRO Commands – Networking & Security

26 ANSI/IEEE Std 802.11, 1999 Edition (R2003), E-ISBN 0-7381-1857-5, 15.4.6.4 Modulation and channel data rates

5.4 Duplex modes for Xbee

The Xbee module use different duplex modes in different parts[27] of the module, a full-duplex UART part and a half-duplex RF part. To connect these two parts of the module a data buffer is used, both for incoming and outgoing data. As earlier specified, in *5.3.4 Data rates*, the RF data rate is twice the UART data rate and this makes the combination of half-duplex and full-duplex less problematic.

5.5 Antenna types

There exists many different forms of antennas, ranging from chip antennas printed on PCB up to big external antennas. This thesis will focus on two types of antennas, *unidirectional* and *omni-directional* (see figures *5.3* and *5.4*).[28]

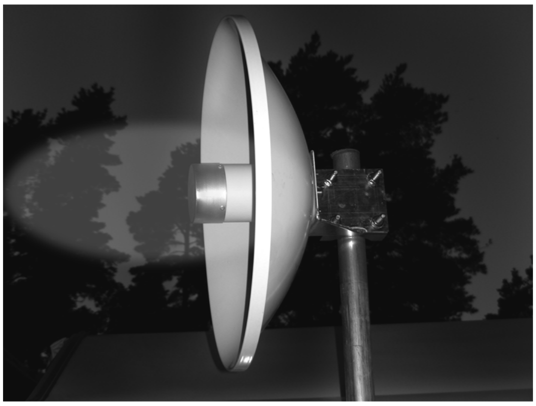

Figure 5.3: Unidirectional antenna (Parabolic)

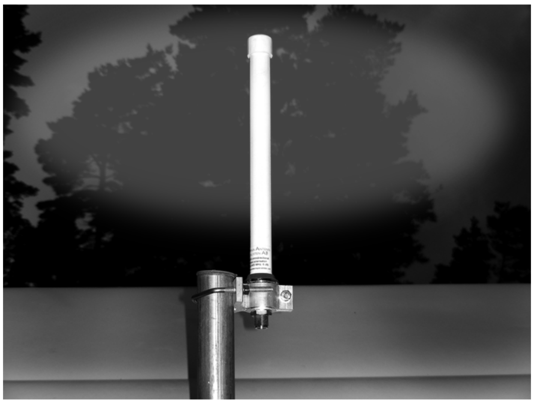

Figure 5.4: Omni-directional antenna

5.5.1 Antenna gain (dBi)

Antenna gain is measured in dBi and specifies the antennas ability to reinforce the RF signal. An antenna with a high gain value reinforces the signal more than an antenna with a low gain value. The dBi value is specifies how much relative gain the antenna has, compared to a perfect isotropic antenna. A perfect isotropic antenna radiates with the same gain in all directions, but it is however only a theoretical antenna used purely for theoretical reasoning.

5.5.2 Unidirectional antenna

This type of antenna is very efficient when sending RF signals over large distances. The RF signal is sent in a very narrow angle, efficiently concentrating the transmit energy to one point. This makes the dBi value high, making it a high-gain antenna. The downside of this is that the antenna has to be physically pointed towards the receiving node, which sometimes is not possible from a practical point of view. Figure 5.3 illustrates how the RF signal is concentrated towards one direction.

27 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13], figure 2-03: Internal Data Flow Diagram
28 Original photos taken by Mats-Åke Wettergren, 2007

5.5.3 Omni-directional antenna

This type of antenna spreads the RF signal 360 degrees (horizontally) around itself. The coverage is however somewhat limited directly below and above the antenna. These characteristics are beneficial when trying to cover a large area with only a single antenna. The downside with this antenna is its limited range, because of the 360 degree spreading of the signal energy. This makes the dBi value low, making it a low-gain antenna. The spreading of the signal energy is illustrated in figure 5.4.

5.6 Swedish National Post and Telecom Agency (PTS)

The Swedish National Post and Telecom Agency (PTS) is the agency that stipulates how radio communication is to take place in Sweden. For this project their specification about maximum Equivalent Isotropically Radiated Power (EIRP) is of great importance. The EIRP value is the limiting factor when the combination of transmit power level and antenna type is chosen.

There exist two different $EIRP_{MAX}$ values for the 2,4 GHz band, one for *spread spectrum* technologies and one for *non-spreading (single channel)* technologies

- For spread spectrum technologies, $EIRP_{MAX}$ = 100 mW (20 dBm)[29]
- For non-spreading (single channel) technologies, $EIRP_{MAX}$ = 25 mW (14 dBm)[30]

The Xbee module uses a spread spectrum technology called Direct-Sequence Spread Spectrum (DSSS) and is therefore limited to $EIRP_{MAX}$ = 100 mW.

5.7 Industrial, Scientific and Medical (ISM)

The Industrial, Scientific and Medical (ISM) band is a collection of frequencies that are license-free to use in almost every part of the world. This project is however limited to Swedish circumstances, so the main concern is Swedish laws and regulation.

ZigBee exists on both the 915 MHz band and the 2,4 GHz band, which both are ISM frequency bands[31]. The 915 MHz band is however only accepted in ITU region 2[32], so for use in Sweden the 2,4 GHz band is the only option.

29 PTSFS 2007:4 - PTS föreskrifter om undantag från tillståndsplikten för vissa radiosändare, ISSN 1400-187X, 5 kap 1 §
30 PTSFS 2007:4 - PTS föreskrifter om undantag från tillståndsplikten för vissa radiosändare, ISSN 1400-187X, 6 kap 2 §
31 ITU Article 5 of the Radio Regulations (Volume 1), 2001, 5.150
32 ITU Article 5 of the Radio Regulations (Volume 1), 2001, 5.4

5.7.1 Limitations

When choosing a combination of an antenna and level of transmitting power special considerations must be taken to ensure that the final system follows PTS' regulations. The maximum EIRP value for the 2,4 GHz band in Sweden is, as earlier stated, 100 mW (20 dBm). To calculate the EIRP value for the combination of transmit power and antenna the following formula (3) can be used:

$$\text{Power of transmitter (dBm)} = \text{Power}_{TX}$$
$$\text{Cable loss (dB)} = \text{Loss}_{CABLE}$$
$$\text{Antenna gain (dBi)} = \text{Gain}_{ANTENNA}$$
$$\textbf{(3)}\ \text{EIRP (dBm)} = \text{Power}_{TX} - \text{Loss}_{CABLE} + \text{Gain}_{ANTENNA}$$

Note: Cable loss (Loss_{CABLE}) is the total amount of signal loss from the transmitter to the antenna (connectors, cables, etc).

For example, in the field test the combination of a Xbee-PRO and an omni-directional antenna has been used. The Xbee-PRO was set up to transmit with +12 dBm and the antenna gain was 2,1 dBi. The cable loss was approximated to 0,1 dB.

$$\text{EIRP} = 12\,\text{dBm} - 0,1\,\text{dB} + 2,1\,\text{dBi} = 14\,\text{dBm}$$

This combination results in a EIRP value of 14 dBm.

6 FIELD TESTS

This chapter describes the field tests that has been performed with the ZigBee modules. The chapter begins with a description of the loopback test and the field test setup. The chapter continuous with some basic facts about the field test, including discussions concerning repeatability, Packet Error Rate (PER) and EIRP issues.

The middle section of this chapter describes the test cases of the field test, with test protocol for each individual test case. The test protocol is divided into four parts, test purpose, expected test result, test procedure and finally the test result. At the end of this section a summary of all test cases is depicted in the form of a table.

The last part of this chapter is focused on range issues, especially indoor and outdoor range limitations. This part also includes a discussion concerning battery powered ZigBee modules.

6.1 Loopback test

This loopback test analyzes loopback data and is the main component of the field test.

The hardware setup consist of a *master* (ATMega162 and a Xbee-PRO module in API mode[33]) and a standalone *slave* (Xbee-PRO in transparent mode[34], with a loopback adapter[35]). When the *master* sends a packet to the *slave* the *slave* immediately sends it back to the *master*. A packet is considered to be lost if the *slave-to-master* packet is not received within *timeout* milliseconds. This *timeout* value can be arbitrary selected to suit different types of loopback tests.

The following parts of the loopback communication are recorded:

- **Number of lost packets:** This value is the number of lost packets that has been recorded by the test.
- **Maximum number of consecutive lost packets:** This value is the maximum number of consecutive lost packets recorded by the test. See *6.3.2.1 Consecutive lost packets* for a more detailed description.
- **Roundtrip time:** The roundtrip time is the time it takes from the point (in code) where the transmit function starts executing until the receive function has finished executing.
- **RSSI value:** Every packet that is received correctly is recorded with a RSSI value. See *4.2.3 Received Signal Strength Indicator (RSSI)* for an explanation of the term RSSI.

For clarity: During the loopback test information about every packet is sent out the serial port. This makes it possible to analyze raw test data off-line, if needed.

33 4.3 API for Xbee
34 Xbee/Xbee-PRO 802.15.4 OEM RF Modules v1.xAx [2006.10.13], 2.1.2 Transparent Operation
35 RX and TX lines connected to each other.

6.2 Field test setup

The field test is based on the loopback test (see *6.1 Loopback test*), with a *master* and a *slave*.

Master:

- One ATMega162 mounted on a STK500 development board.
- One Xbee-PRO mounted on a Xbee development board, connected with the ATMega162 via RS-232.
- Transmit power level: +12 dBm.
  Antenna: Omni-directional with 2,1 dBi gain, connected to the Xbee-PRO via a pigtail adapter[36].
- Firmware: IEEE 802.15.4 version 1.0.A.3.
- One PC connected to the ATMega162 via RS-232.

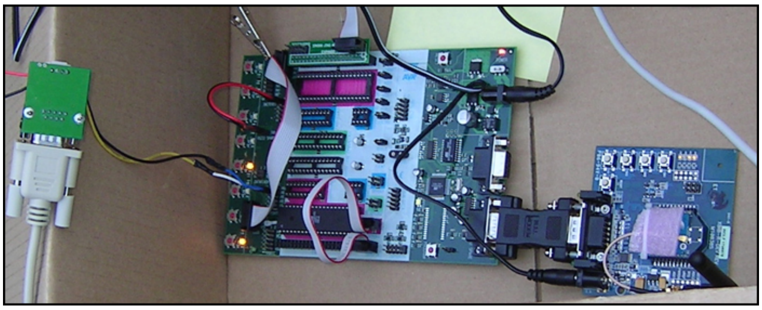

Figure 6.1: Master (loopback test)

Slave:

- One Xbee-PRO mounted on Xbee development board, with a loopback adapter.
- Transmit power level: +12 dBm.
  Antenna: Omni-directional with 1,5 dBi gain, connected to the Xbee-PRO directly (whip antenna).
- Firmware: IEEE 802.15.4 version 1.0.A.3 *(slave)*.

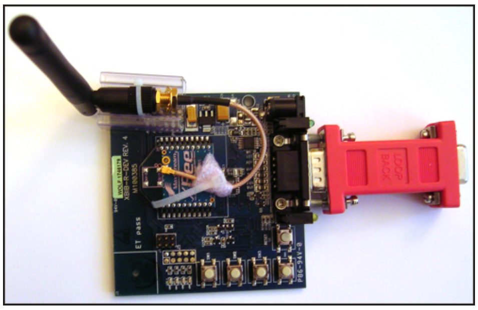

Figure 6.2: Slave (loopback test)

36 A pigtail adapter makes it possible to connect mismatching connectors.

The Xbee-PRO module was selected because of its superior wireless performance compared to the Xbee-STD module. The omni-directional antenna type was chosen in favor of the unidirectional antenna type because it suits the product from Binar in a better way.

The loopback test is configured to send 20 000 packets at a baudrate of 115,2 kbit/s. The data payload (frame data) is 8 bytes and the timeout value for a lost packet is 21 ms. During the test raw test data is sent out the serial port to the PC where it is logged to file on the PC's hard drive. When the test has finished it outputs the test results to the PC in the same way as raw data has been sent earlier. The test takes around 10 minutes to complete.

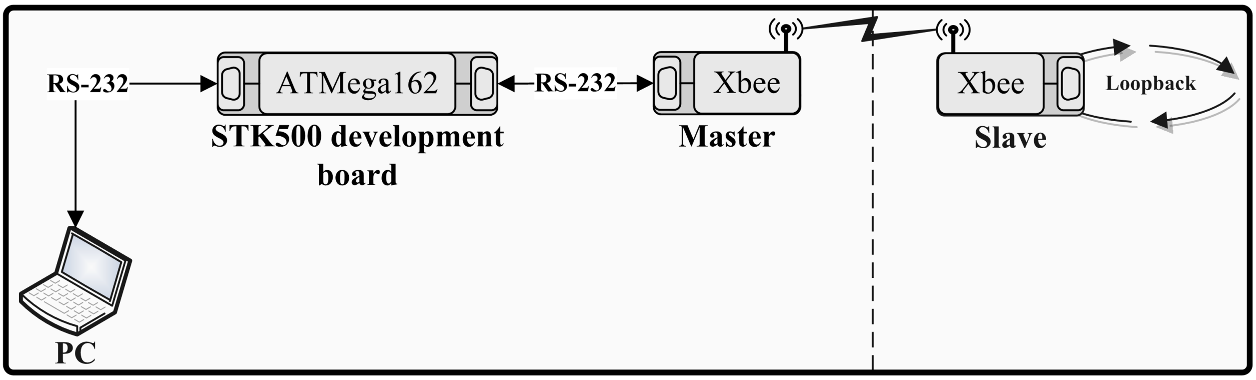

Figure 6.3: Field test setup (loopback test)

6.3 Field test basics

This section explains some basic facts concerning the field test.

6.3.1 Repeatability

In order to get reliable test results every field test is repeated three times. The three tests is performed one after another with no more than five minutes in between. This procedure compensates for any deviant conditions during the test period.

6.3.2 Packet Error Rate

The Packet Error Rate (PER) is calculated as follows:

$$\mathrm{PER} = \frac{\text{Number of lost packets}}{\text{Total number of packets}}$$

A PER value that is under 1% is considered to be an acceptable[37] level for this type of communication.

37 IEEE Std. 802.15.4-2003, ISBN 0-7381-3677-5, Annex E.2.2 Modulation

6.3.2.1 Consecutive lost packets

The PER value can, in some cases, be misguiding when using the value as a measurement of how reliable the communication is. The reason for this is that the PER value does *not* take into account the number of consecutive lost packets during a test session. The following case study describes the issues concerning the PER value:

Case study on PER value:

Two test sessions has been recorded, with a total number of 100 packets sent for each session. The results from the two test sessions is depicted in table 6.1.

Table 6.1: PER example

	1	**2**
PER	0,07%	0,07%
Number of consecutive lost packets	7	1

The PER value from both sessions is the same, but there is a significant difference between them, namely the number of consecutive lost packets. A high[38] number of consecutive lost packets has negative effects on communication reliability, especially for time-critical communication. The negative effects for time-critical communication is manifested in violated time constrains, due to a large number of consecutive lost packets.

For systems without time constraints the number of consecutive lost packets is of no concern, as long as the data payload eventually gets to it destination.

6.3.3 EIRP effects

These tests were performed according to PTS[39] limitations for a *non-spreading* technology. After these tests were performed it was discovered that the Xbee in fact *does* use a *spread spectrum* technology. This mean that a higher EIRP value could have been used for the tests, with a stronger signal at the receiver as a consequence. A stronger signal at the receiver makes it easier for the receiver to interpret the signal correctly, especially when noise interfere with the signal. It is however a marginal difference between a strong and a weak signal when no significant noise interfere with the signal.

The field tests were some sort of a active noise-source interfere with the test signal are the following: *Microwave oven*, *Bluetooth®*, *ZigBee*, *Industry environment* and *Industry robot.* These test should benefit from a higher EIRP value, with slightly less packets lost as a result. The other tests should however not result in less packets lost, as a result from an increased EIRP value.

38 The threshold for a high value is application specific.
39 5.6 Swedish National Post and Telecom Agency (PTS)

6.4 Test cases

This section describes the different test cases and ends with a summary of the test results. The different test environments was chosen with concern to what materials and noise-sources a ZigBee device would most likely come across in an industrial environment.

6.4.1 Office wall

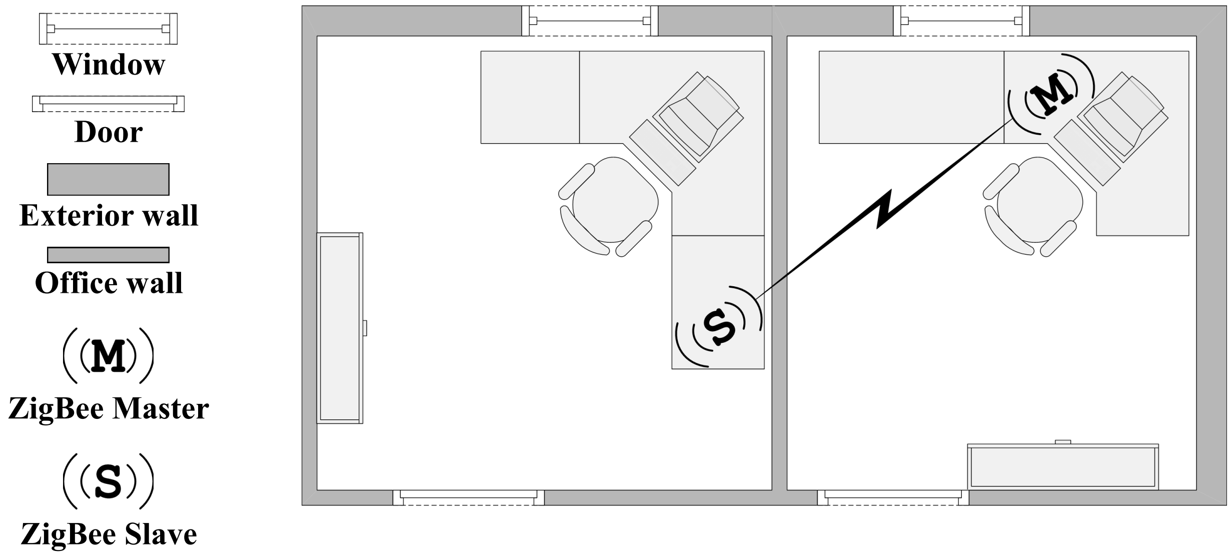

Figure 6.4: Office wall

Test purpose: The purpose of this test was to see how the signal was affected when being sent through an office wall.

Expected result: No significant effects on the signal is expected, only a slight decrease of the signal strength.

Test procedure: The test signal was sent through a typical office wall, approximately 15 centimeter thick. Although no intentional source of interference was deployed in the surroundings there was some minor interference from Bluetooth® and WLAN equipment. These additional sources of interference should however not affect the test result as the ZigBee signal was much stronger than the interfering signals.

Test result: Test result as expected.

6.4.2 Sheet metal wall

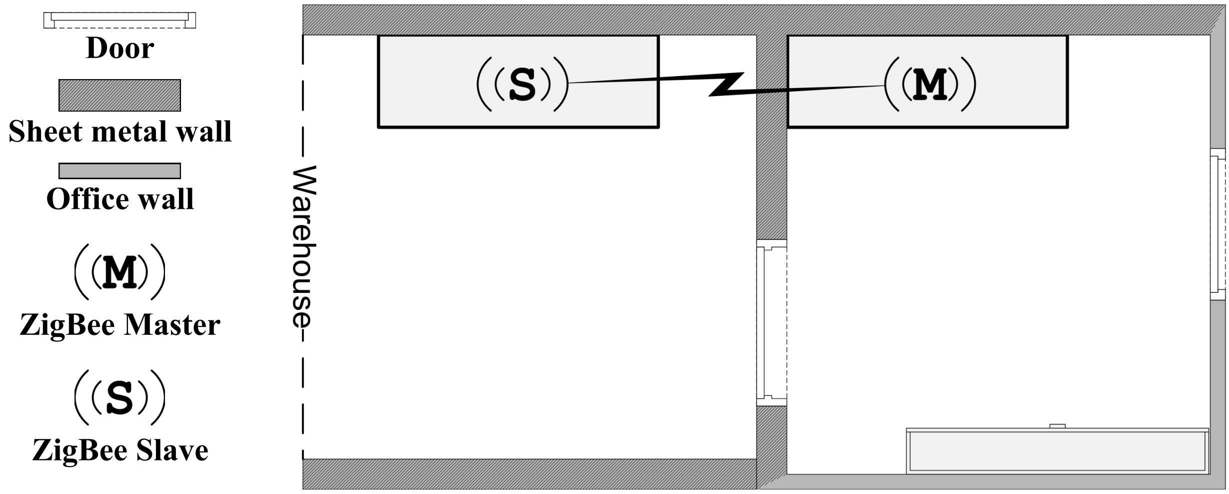

Figure 6.5: Sheet metal wall

Test purpose: The purpose of this test was to see how the signal was affected when being sent through sheet metal.

Expected result: The signal should not be able to penetrate the sheet metal due to the shielding effects of the material.

Test procedure: The test signal was sent through a wall that had one side covered with sheet metal. The total thickness of the wall was approximately 25 centimeter. The RF environment was considered interference free.

Test result: The test signal was received at the slave node, and sent back to the master without any major problems. The signal strength was however the lowest of all test cases, indicating that the sheet metal attenuated the signal significantly.

This unexpected result is probably due to the following reasons:

- The signal found its way through the sheet metal at the joints of the wall.
- The signal was reflected by the joist in the ceiling, and by that effectively circumventing the shielding effects from the wall.

For further testing it is recommended that test environment is chosen with concern to the new-found problems described above.

6.4.3 Bluetooth

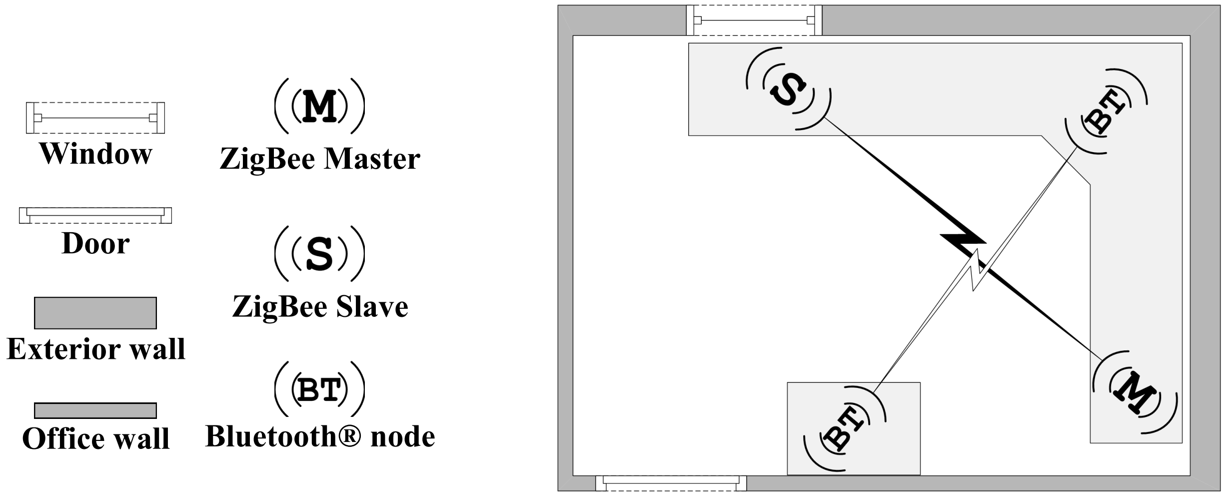

Figure 6.6: Bluetooth

Test purpose: The purpose of this test was to see how the signal was affected by Bluetooth® communication.

Expected result: The signal is expected to have problems with interference from the Bluetooth® communication. This will increase the PER value and the number of consecutive lost packets.

Test procedure: This test was performed with Bluetooth® traffic in the direct vicinity of the Xbee nodes. The Bluetooth® traffic was generated from two Bluetooth® modules that was performing a loopback test. All nodes was placed inside a radius of approximately two meters.

Apart from the above test signals there was also WLAN/Bluetooth® equipment deployed in the surroundings. This WLAN/Bluetooth® equipment should however only have a marginal effect on the test result as the test signals was much stronger than the WLAN/Bluetooth® signals.

Test result: The test result was unexpected as the PER value was very low, actually the lowest of all test cases! The number of consecutive lost packets was also within reasonable limits. This result shows that interference from Bluetooth® traffic should not be a problem when using the Xbee modules.

6.4.4 ZigBee loopback

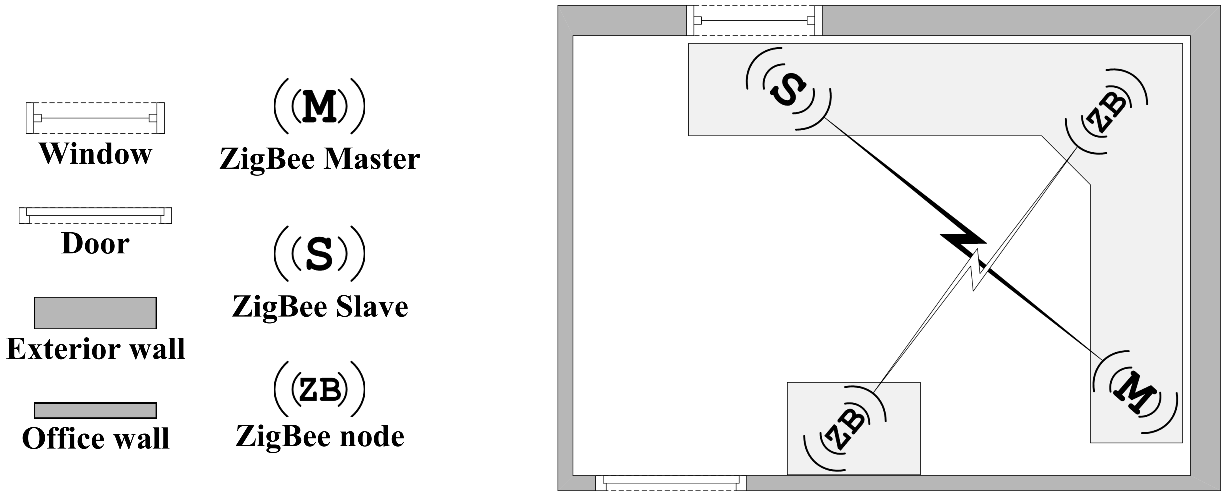

Figure 6.7: ZigBee loopback

Test purpose: The purpose of this test was to see how the signal was affected by another ZigBee signal.

Expected result: The signal is expected to have minor problems with interference from the extra ZigBee communication. This will result in a slight increase of the PER value, from the extra interference. However, because the two competing signals is using the same protocol they should be able to share the available bandwidth, without any significant increase of consecutive lost packets.

Test procedure: This test was performed with two additional Xbee-STD nodes, apart from the master node and the slave node. These two additional Xbee-STD nodes was used to generate ZigBee interference traffic, through another loopback test. In order to increase the interference all Xbee nodes was configured to work on the same channel. All nodes was placed inside a radius of approximately two meters.

Apart from the above test signals there was also WLAN/Bluetooth® equipment deployed in the surroundings. This WLAN/Bluetooth® equipment should however only have a marginal effect on the test result as the test signals was much stronger than the WLAN/Bluetooth® signals.

Test result: The test result was unexpected concerning the PER value of 3,64%, it was much higher than expected. The PER value was also the highest of all test cases, but it did however not have a large number of consecutive lost packets. The low number of consecutive lost packets could be explained by the CCA used by the Xbee nodes, but this is something that needs to be verified by further testing.

The reason for the high PER value is most likely due to the usage of the same channel for all traffic, in combination with the nearness of the nodes. It is probable that the interference due to concurrent ZigBee traffic would decrease as the nodes are moved further away from each other. Another way of improving the communication is to select channels in a way that minimizes overhearing between channels (see section *5.3.3 Spread spectrum side-effects on channel usage*).

6.4.5 Microwave oven

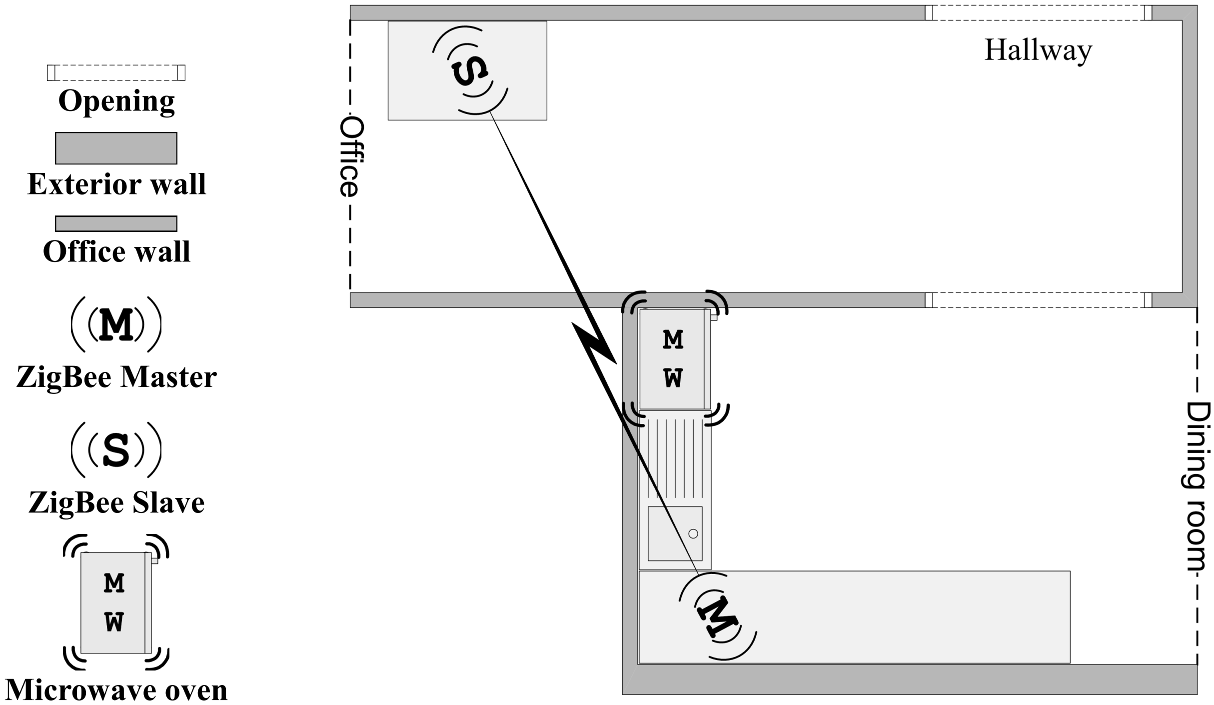

Figure 6.8: Microwave oven

Test purpose: The purpose of this test was to see how the signal was affected by an active microwave oven.

Expected result: The signal is expected to have significant problems with interference from the microwaves that leak from the microwave oven. This will significantly increase the PER value and the number of consecutive lost packets.

Test procedure: This test was performed with a standard microwave oven that was placed in between the master node and the slave node. The distance between the two nodes was approximately 10 meters. The microwave oven[40] was set to maximum power during the whole test.

Apart from the above test signals there was also WLAN/Bluetooth® equipment deployed in the surroundings. This WLAN/Bluetooth® equipment should however only have a marginal effect on the test result as the test signal was much stronger than the WLAN/Bluetooth® signals.

Test result: The test resulted in a PER value under 1%, significantly lower than expected. The PER value was however the second highest PER value of all test cases, which indicates a small increase of interference compared to the other test cases.

But, as discussed in *6.3.2.1 Consecutive lost packets*, the PER value is not the only factor. The number of consecutive lost packets in this test was 15, the highest of all test cases. This indicates that microwave ovens is a potential threat for time-critical communication.

40 Whirlpool MD113/WH

6.4.6 Industry environment

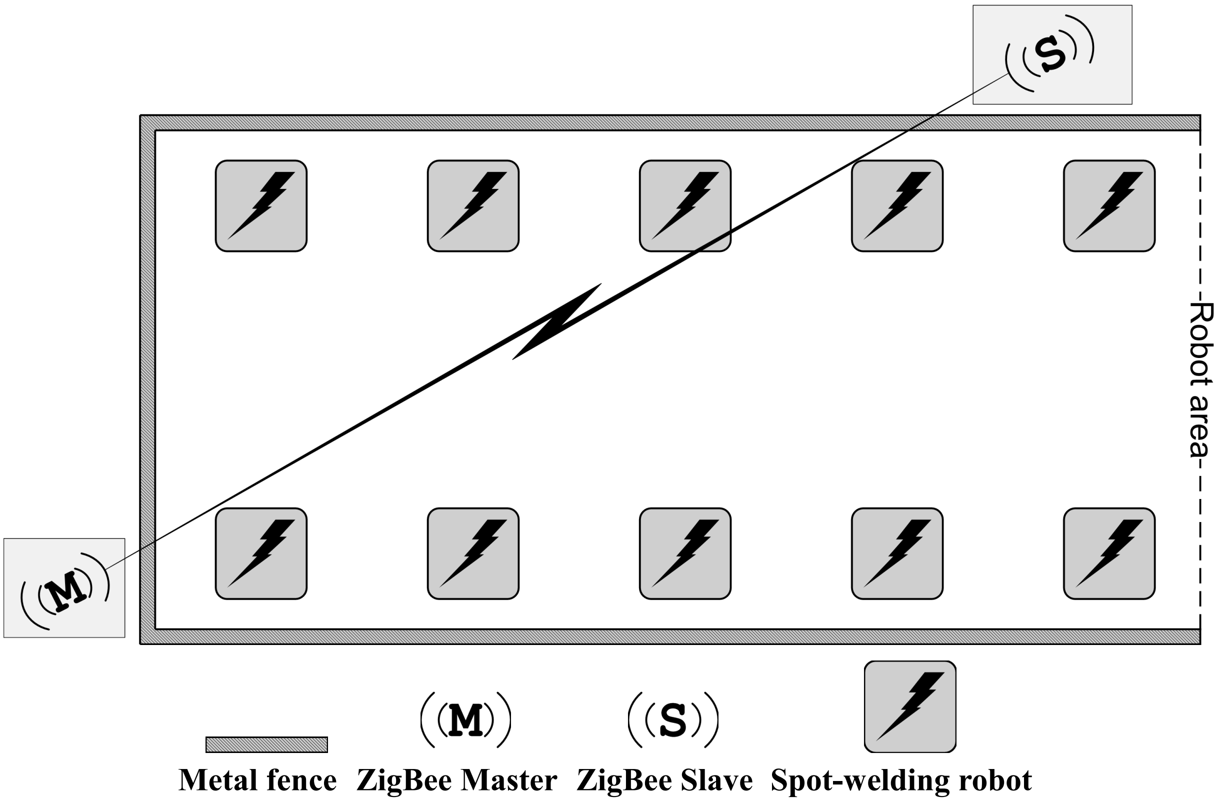

Figure 6.9: Industry environment

Test purpose: The purpose of this test was to see how the signal was affected in an industry environment.

Expected result: The signal is expected to have problems with interference from the industrial environment, for example high-frequency noise from welding machines. This will increase the PER value and the number of consecutive lost packets.

Test procedure: This test was performed by placing the master node and the slave node in an industry environment with spot-welding robots. The distance between the nodes was approximately 20 meters. The test was performed during normal operation of the robots.

Test result: The test resulted in a PER value of 0,44% which is considered an acceptable value as it is under 1%. The number of consecutive lost packets was 7, a medium-high value compared to the other test cases. This medium-high number indicates that there might be a problem satisfying the time constraints for time-critical communication.

6.4.7 Industry robot

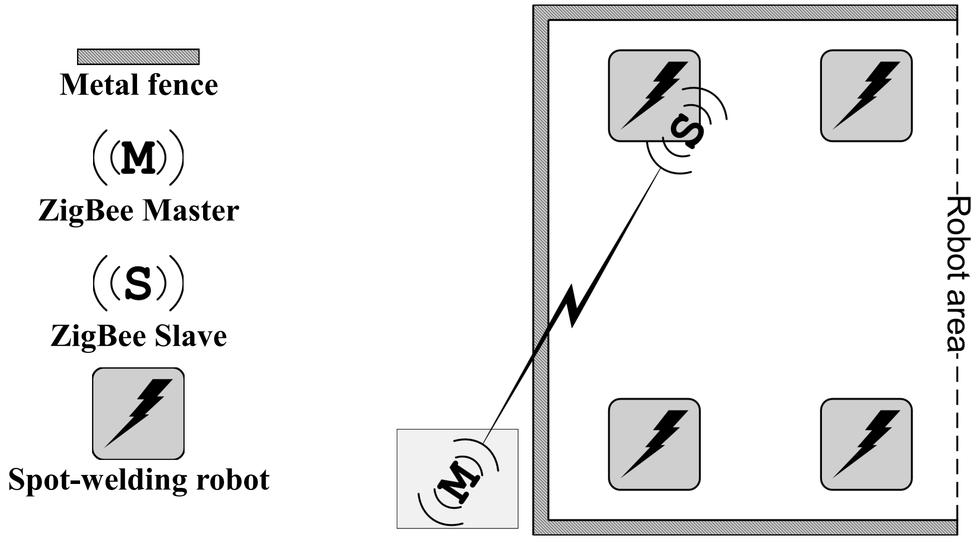

Figure 6.10: Industry robot

Test purpose: The purpose of this test was to see how the signal was affected when the slave node was mounted on an industry robot that was used for welding.
Expected result: The signal is expected to have significant problems with interference from the industry robot and its welding equipment. The PER value and the number of consecutive lost packets should be higher than for *6.4.6 Industry environment.* The reason for this is that the slave node is mounted closer to the welding equipment than in 6.4.6.

Test procedure: This test was performed by mounting the slave node on an industry robot that was used for spot-welding. The master node was placed approximately 5 meters from the slave node. During the test the robot was working in normal production mode.

Test result: The PER value was 0,15% and the number of consecutive lost packets was 2. This result was unexpected as the result from 6.4.6 showed higher values. The reason for this unexpected result is hard to explain without further testing, but one possible explanation could be the difference in distance between the nodes. The longer distance in 6.4.6 made the signal weaker than in this test, which in return made the signal in 6.4.6 less robust when being exposed to interference.

6.4.8 Noise-free environment

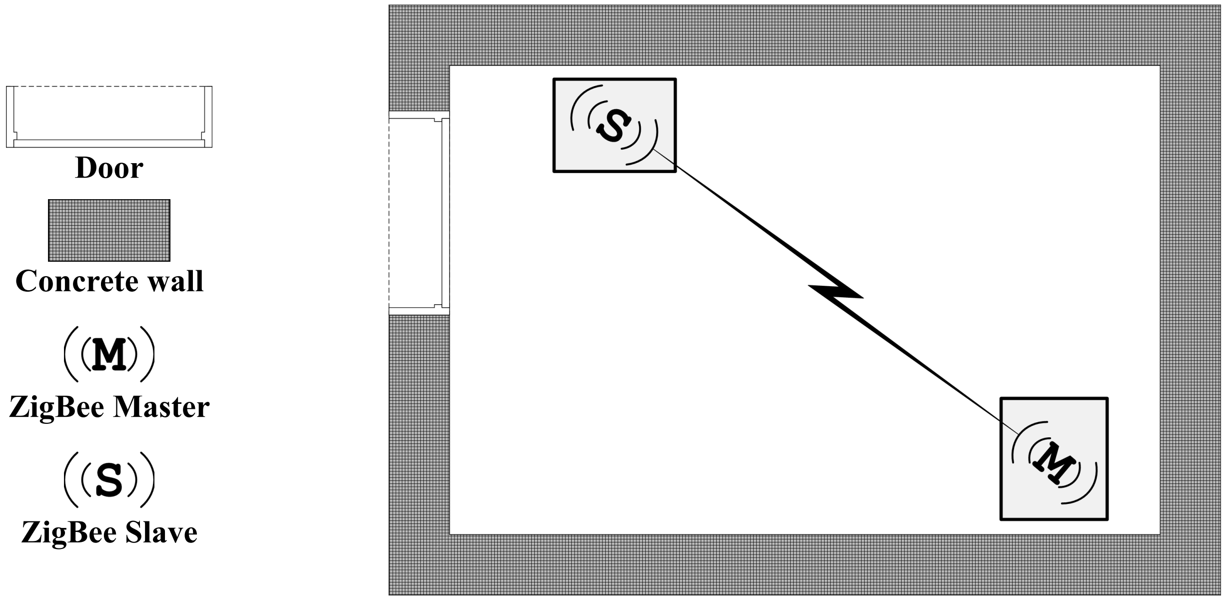

Figure 6.11: Noise-free environment

Test purpose: The purpose of this test was to see how the signal was affected in an isolated noise-free environment.

Expected result: The signal is expected to have no problems with interference because of the noise-free environment. The PER value and the number of consecutive lost packets should be the lowest of all test cases. The result from this test should be a good reference level for a noise-free environment.

Test procedure: This test was performed inside a bunker (air-raid shelter). The master node and the slave node was placed approximately 10 meters apart.

Test result: The packet error rate was 0,29% and the number of consecutive lost packets was 5, a medium-high value in this context. This was much higher values than expected for this environment, especially as one would imagine that a bunker would be practically noise-free due to the isolation from noise sources. This assumption was however not confirmed with measurements, so it is possible that that there were more noise than expected in the environment. Another plausible explanation for the high values is an increase of radio reflections in this confined space.

6.4.9 Summary of results

The results from the field tests is depicted in table 6.2. The most notable figures in the table are marked in bold.

Table 6.2: Summary of field test results

	Office wall	Microwave oven	Sheet metal wall	ZigBee loopback	Bluetooth	Industry env.	Industry robot	Noise-free env.
Lost packets (average)	20,67	152,33	24,67	727,67	8	87,67	30,67	58,67
Max consecutive lost packets	2	**15**	2	3	2	7	2	5
Roundtrip typical (ms)	15	15	15	15	15	15	15	15
RSSI typical (dBm)	−44	−57	−72	−50	−48	−59	−53	−70
Packet Error Rate (PER)	0,10%	0,76%	0,12%	**3,64%**	0,04%	0,44%	0,15%	0,29%
Packet count	20 000	20 000	20 000	20 000	20 000	20 000	20 000	20 000

Observations:

- The RSSI value does *not* affect the PER value, nor the number of consecutive lost packets. The underlaying reasons for this behavior can be explained by the discussion in *5.2 Receiver sensitivity*.
- The only test case that had a PER value above 1% was the ZigBee loopback. This indicates that their *might* be a problem using a large number of concurrent ZigBee nodes side by side. This is however something that needs to verified by more extensive field tests before any well-founded conclusions can be drawn concerning this particular problem.
- A microwave oven should not be underestimated when considering possible sources of noise.
- The results from the two tests that were performed in an industrial environment show that there should be no major problems using ZigBee in such an environment.
- The roundtrip time is the same for all test cases, indicating that the roundtrip time is independent of the environment.

6.5 Range tests

This section describes range limitations for the Xbee module. The maximum range has been measured with loopback testing, using the Xbee-PRO module configured according to *5.7.1 Limitations*. A node is considered to be *in-range* when the loopback data is transmitted correctly between the base station and the loopback node. Respectively is a node considered to be *out-of-range* when loopback data is lost.

6.5.1 Range test setup

The range test was performed with a software from MaxStream called X-CTU. The software has a basic loopback test that only require the Xbee module combined with the Xbee development board. This has the advantage that the test is easier to perform, as no external microcontroller is needed. The baudrate used was 115,2 kbit/s, the same as for the field tests.

The following hardware setup was the used for the test:

Master:

- One Xbee-PRO connected to the PC via USB.
- Transmit power level: +18 dBm.
  Antenna: Omni-directional with 1,5 dBi gain, connected to the Xbee-PRO directly (whip antenna).
- Firmware: IEEE 802.15.4 version 1.0.A.3.

Slave:

- One Xbee-PRO with a loopback adapter.
- Transmit power level: +18 dBm.
  Antenna: Omni-directional with 2,1 dBi gain, connected to the Xbee-PRO via a pigtail adapter.
- Firmware: IEEE 802.15.4 version 1.0.A.3.

6.5.2 Test results

The indoor test was performed in an office environment, with the signal going through several walls. The walls in this test was thicker than the wall in *6.4.1 Office wall*, thus making the thicker wall attenuate the signal more than the wall in *6.4.1*.

The outdoor test was performed in a residential district with visual line-of-sight between the two nodes. The test results is depicted in table 6.3.

Table 6.3: Maximum range

	Indoor	**Outdoor**
Maximum range	30 m	500 m

These test results shows that the maximum range differs significantly in different types of environments, with more than ten times longer outdoor range, compared to the indoor range. It should however be noted that the maximum range most likely would increase if unidirectional antennas is used instead of omni-directional.

Note: In the documentation[41] from MaxStream the Xbee-PRO module is specified to a maximum indoor range[42] of 43 meters and a maximum outdoor range[43] of 1335 meters. The difference between the results in this thesis and MaxStream's results is possibly due to a more ideal test environment for MaxStream's measurements.

6.5.2.1 Low voltage issues

During these range tests a battery powered Xbee module has been used as the loopback device. This worked fine in the beginning, but in the end, when the battery voltage dropped, the signal barely reached the base station from a distance of one (1) meter. This indicates that is important to have a reliable power source when using the Xbee.

6.5.3 Battery life and energy consumption

This section handles the questions about battery life and energy consumption.

6.5.3.1 Discussion

The energy consumption has a strong relation to how often the ZigBee module receives and transmits data. In the case of the Xbee the energy needed for transmitting depends on the chosen power level. The energy for receiving is fixed and stays the same regardless of what the transmit power level is set to.

The energy consumption is consequently dependent on how much traffic each node has to handle. For example, if a battery powered ZigBee device only transmits and receives once every hour, for instance a light switch, the battery in this device will be drained very slowly. On the other hand, a system that communicates with the ZigBee device once every second to check if the device is still alive will drain the battery significantly faster.

6.5.3.2 Conclusion

It should be possible to have a ZigBee device that is battery powered. However, the question about how often the battery must be changed is highly dependent on how the much ZigBee communication is needed to and from the device.

41 MaxStream Application Note XST-AN019a, September 2005
42 In an office environment
43 With visual line-of-sight

7 Conclusions

The ZigBee technology is clearly on the uprise and will most likely be used more often in the future, especially for industry applications and consumer electronics. The combination of low-cost hardware, very good radio performance and a global standard (ZigBee Alliance) makes ZigBee a competitive choice on the wireless market.

7.1 Appropriate for industrial usage?

The research and test results from this project has clearly shown that ZigBee, and Xbee in particular, has a potential to satisfy the requirements for a wireless system in an industrial environment. This conclusion concerning the industrial usability of ZigBee should however be seen in the light of this particular project, making this conclusion viable only for the field test environments. When considering untested environments there are no test results to draw conclusions from, but an educated guess is that ZigBee probably will perform well in most cases, making it a good choice for industrial usage.

8 FURTHER WORK

In order to simplify further work a few suggestions is listed below:

- More extensive field tests concerning concurrent ZigBee traffic. (See observations from *6.4.9 Summary of results*.)
- Practical tests to see the effects of overhearing between channels. (See *5.3.3 Spread spectrum side-effects on channel usage*.)

APPENDICES

A CODE LISTING

See attached CD-ROM or the thesis webpage, located at the URL below:
http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-10061

B Requirement specification

Theoretical task

Requirement/desired specifications:

- Should work in an industry environment.
- Temperature range from –20 °C up to +60 °C.
- Multiple systems must work side by side, independent of each other. This also applies to unknown systems that is out of Binar's control.
- Number of nodes in the same system: 100 (preferably more).
- Number of nodes in the same area: 5000 (preferably more).
- Data rate when reading strings: 100 byte/second (preferably corresponding to 9600 baud).
- No data is allowed to be lost.
- The system should notice if the communication with the master/slave nodes is lost (within a few seconds).
- It should be easy to replace a broken end node with a new end node.
- Response time requirements: When a button has been pressed it must be noticed by the system within 100-200 milliseconds.
- It should be possible to update the firmware in the ZigBee nodes over-the-air.

Questions:

- Which frequency band should be used with ZigBee? Advantages / Disadvantages? What should we use?
- Markets: Where is it allowed to use the different frequency bands? Is there geographic limitations? What are the limitations in different types of industry environments?
- Robustness against interference: Our system must work side by side with microwave ovens, RFID antennas, etc. Is this a sensitive issue and how does one solve it?
- Range? Is there a need for a repeater?
- Different antennas: What is needed, which types exist, which type should be used?
- Is virus in these kind of system a reality? In the case of existing viruses, what protection should be used?
- Power consumption: What is the minimum power consumption for a working system?
- Market research, which suppliers of ZigBee components is there? Component prices?
- Range: What is the range of the system?
- Certification: Is it obligatory? Cost? Benefits?
- Is it possible to use other ZigBee products in our system?

C MARKET RESEARCH TABLE

ZigBee Chip											
Manufacturer	**ZigBee-version**	**Stack**	**Mesh**	**Positioning**	**Frequency band**	**Chip**	**Price***	**Encryption**	**Receiver Sensitivity**	**Transmit Power (Max)**	**Comments**
Chipcon / Texas Instruments	2006	Z-stack	Yes	Yes (Beta version)	2,4 GHz	CC2420/30/31	$6	Hardware-AES	−95 dBm (CC2420)	0 dBm (CC2420)	Location engine in beta version
Ember	2004	EmberZNet	Yes	No	2,4 GHz	EM250/260	$7	Hardware-AES	−98 dBm (EM260)	+5 dBm	
Freescale	2004	Z-stack	Yes	No	2,4 GHz	MC1319x,MC1320x,MC1321x	$4	Software-AES	−92 dBm (MC1321x)	+3 dBm (MC1321x)	
Helicomm	2004	Helicomm Stack	Yes	No	915 MHz / 2,4 GHz	IP-Link 1000/122x	$25	AES	−94 dBm (IP-Link 1220)	+10 dBm (IP-Link 1220)	Probably hardware-AES
Jennic	2004	WiniZB Stack	Yes	No	2,4 GHz	JN5121/513x	£20	Hardware-AES	−97 dBm (JN513x)	+3 dBm (JN513x)	
MeshNetics	2006	eZeeNet Stack	Yes	No	2,4 GHz	ZDM-A1281-xx	$21	Software-AES	−101 dBm (ZDM-A1281-xx)	+3 dBm (ZDM-A1281-xx)	
Microchip Inc.	2004	Microchip Stack	Yes	No	2,4 GHz	MRF24J40	$3	Hardware-AES	−91 dBm (MRF24J40)	0 dBm (MRF24J40)	
OKI Semiconductors	2006	OKI-stack (unconfirmed)	Yes	No	2,4 GHz	ML7065	$4	Hardware-AES	−90 dBm (ML7065)	+3 dBm (ML7065)	Probably OKI-stack
RadioPulse Inc.	2004	RadioPulse Stack (unconfirmed)	Yes	No	2,4 GHz	MG2400/LM2400	$10	Hardware-AES	−99 dBm (LM2400)	+14 dBm (LM2400)	Probably zPULSE-stack

Price*: Average price from random supplier

ZigBee Products											
Manufacturer	**ZigBee-version**	**Stack**	**Mesh**	**Positioning**	**Frequency band**	**Product name (chip)**	**Price***	**Encryption**	**Receiver Sensitivity**	**Transmit Power**	**Comments**
Integration UK	2006	Integration ZigBee Stack	Yes	No	2,4 GHz	IA OEM-DAMD1 2400 (OKI ML7065)	$49	Hardware-AES	−90 dBm	0 dBm	USB version available
MaxStream	2004	Z-stack	Yes	No	2,4 GHz	Xbee (MC13193)	$19	Hardware-AES	−100 dBm (Xbee-PRO)	+18 dBm (Xbee-PRO)	
Renesas	2006	Renesas Stack	Yes	No	2,4 GHz	RZB-CC16C-ZDK (Chipcon / ZMD)	N/A	N/A	N/A	N/A	Radio module is customer selectable. 900 MHz version is under development

ZigBee stack only											
Manufacturer	**ZigBee-version**	**Stack**	**Mesh**	**Positioning**	**Frequency band**	**Compliant chips**	**Price**	**Encryption**	**Receiver Sensitivity**	**Transmit Power**	**Comments**
Korwin	2004	WiniZB Stack	Yes	No	2,4 GHz	JN5121/CC2420	N/A	N/A	Chip dependent	Chip dependent	
Institute for Information Industry	2004	III ZigBee IZAP/SCC	Yes	Yes	2,4 GHz	CC2430/JN5121	N/A	N/A	Chip dependent	Chip dependent	
AirBee	2006	Airbee ZNS 2006	N/A	N/A	N/A	N/A	N/A	N/A	Chip dependent	Chip dependent	Depends on chip/stack selection

Price*: Average price from random supplier